

## Half of businesses unaware if staff are running virtual desktops, Sophos poll reveals unmanaged virtual computers can threaten corporate IT security

21 October 2008

Sophos's Richard Jacobs says companies need to be aware of the security issues surrounding virtualization.

IT security and control firm Sophos has announced that the application control feature of Sophos Endpoint Security and Control has been extended to give businesses the option to block virtualization applications, including free desktop and data centre products from VMware, as well as tools from DosBox and Microsoft's Virtual PC 2007. The growing popularity of virtualization tools and the ease with which they can be downloaded means that there is a much greater risk of end-users creating a virtual environment in which to run unauthorized applications, from games to browsers to beta software.



While virtualization can represent real value at this time of increasingly constrained IT budgets, Sophos notes that IT administrators must prioritize management of these virtual desktops, as unmanaged virtual computers can open holes in an organization's security system. However, a recent Sophos poll\* has revealed that more than half of all businesses do not know how many employees are running virtualization software on their computers.

"Virtualization tools represent a black hole in many organizations' IT security – if staff are allowed to download these tools and create environments that are completely hidden from IT administrators, it's impossible to defend them against cyber attacks," said Richard Jacobs, chief technology officer at Sophos. "While employees may simply be trying to get round a ban on social networking or using instant messaging at work, doing so in this way poses a real threat. In fact, uncontrolled and unmanaged virtual computers could lead to potentially disastrous consequences, including corporate identity theft, financial losses and embarrassing headlines."

Sophos notes that as more and more employees have considerable IT knowledge, it is vital that businesses have complete visibility of the corporate network. This is especially important given the growth in the number of free virtualization tools on the market – while employees may be downloading them with no malicious intent, the ability to run whatever they choose on their virtual desktop means that the company may be facing cyber risks unbeknown to anyone in the organization. For example, an unauthorized virtual browser may not be up to date with security patches giving hackers a potential vector of attack, or the user may be running unprotected peer-to-peer (P2P) programs virtually.

To overcome this, Sophos recommends that companies ensure that employees are not only aware of the firm's acceptable usage policy, but that IT staff also have visibility into which applications staff are downloading and using. By effectively managing and securing the virtual environment, businesses can enjoy the benefits of virtualization without the associated risks.

"By enabling organizations to reduce the amount of hardware they need, virtualization can offer real cost-saving benefits – especially important in the public sector," said Antony Barke, senior technical engineer at Basildon and Thurrock University Hospitals NHS Foundation Trust, a Sophos customer. "However, it's essential to secure the virtual environment, just as you would the rest of the corporate network – the same threats exist and this shouldn't be overlooked. With the right security measures, virtual machines are a real asset to the network, rather than a potential liability."